



Australian Government

Department of Finance and Administration

Australian Government Information Management Office

Department of Finance and Administration

**Australian Government Information Management
Office**

Implementation Guide for Email Protective Markings for Australian Government Agencies

October 2005

Version: 1.0
Date: 1 October 2005
Sponsor: Australian Government Information Management Office
Author: Geoff Morrison

© Commonwealth of Australia 2005

COMPLIANCE WITH THE PSM AND ACSI 33

The Australian Government Information and Communications Technology Security Manual (ACSI 33) (September 2005) at 3.5.46 states that ‘the standard for the application of protective markings to emails will be promulgated separately once it has been finalised.’

The Implementation Guide for Email Protective Markings for Australian Government Agencies Version 1 (October 2005) and the Email Protective Marking Standard for the Australian Government Version 1 (October 2005) were developed to assist agencies in implementing protective markings. These documents can be accessed at www.agimo.gov.au.

The Defence Signals Directorate (DSD) has reviewed these documents for consistency and compliance with ACSI 33 (September 2005) and the ICT Security Policy for the Use of BlackBerry by the Australian Government (July 2005). DSD supports the use of these documents by agencies in the implementation of protective markings in an agency environment. Compliance with these documents will ensure agencies manage and protect Australian Government information in accordance with the protective marking requirements of the PSM and ACSI 33.

In addition, DSD also considers that such an agency implementation will assist agencies to comply with the whole-of-government policy on BlackBerry as promulgated by AGIMO.

Table of Contents

Table of Contents	ii
Table of Figures	iii
List of Tables	iii
Reference Documents	iv
Document Revision History	v
1 Introduction	1
1.1 Scope	4
1.2 Timing	4
1.3 Implementation Path	5
1.4 Intended Audience	6
1.5 Assumptions	6
1.6 Protective Marking Implementation Discussion Forum	6
1.7 Contacts	7
2 Background	8
2.1 Email Headers	8
2.2 Protective Marking Standard for Email	8
3 Email Policy and User Awareness Guidelines	10
4 Email Clients	11
4.1 ‘No Default’ Protective Marking	11
4.2 3 rd Party Products	11
5 Email Architecture	13
6 Email Server Considerations	16
6.1 Server Behaviour Rules	16
6.1.1 Email Originating from Outside of the Australian Government	16
6.1.2 Outbound email (sending)	17
6.1.3 Inbound email (receiving)	22
6.1.4 Forwarding email (receive and send)	27
6.1.5 Summary – Server Behaviour Rules	30
6.2 FedLink Lookup Table	32
6.3 Private Link Lookup Table	32
6.4 Email Blocking and Logging	32
6.5 Gateway Translation	33
6.6 Error Conditions	33
6.7 Server Performance and Testing	34
6.8 Staggered Implementation of Protective Markings	34
7 System Generated Email	37
8 Remote and Mobile Access to Email	37
Appendix A – Sample Acceptable Use Email Guidelines	38
Policy Statements	38
User Guidelines	38
Appendix B – Sample Email Rejected Messages	42
Outbound Message	42
Inbound Message	42
Appendix C – Glossary of Terms	44

Table of Figures

Figure 1 - Relationship between national policy, email protective marking policy, metadata standard and implementation guide.....	3
Figure 2 - Email headers and message body.....	8
Figure 3 - High level email transmission paths	14
Figure 4 - Detailed email architecture	15
Figure 5 - Outbound email.....	17
Figure 6 - Inbound email.....	22
Figure 7 - Auto forwarding of email to BlackBerry device.....	27
Figure 8 - Recipient forwarding of email	29

List of Tables

Table 1 - 3rd Party email client and content filtering products	12
Table 2- Outbound email, defined permitted security classifications.....	19
Table 3 - Outbound email server rules.....	21
Table 4 - Inbound email, defined permitted security classifications	23
Table 5 - Inbound email server rules	26
Table 6 - Email flow, auto forwarding to BlackBerry device.....	28
Table 7 - Email flow, manual forwarding of email	30
Table 8 - Email transfer route key (used in Table 9)	30
Table 9 - Summary server behaviour actions (deliver or reject)	31
Table 10 - Example FedLink table for outbound and inbound email	32
Table 11 - Blocked email notification and logging	32
Table 12 - Extended FedLink lookup table, showing the status of the implementation of protective markings	36
Table 13 - Glossary of Terms	45

Reference Documents

1. Commonwealth Protective Security Manual 2005
Attorney-General's Department
<http://www.ag.gov.au/www/protectivesecurityhome.nsf>
2. Australian Government Information and Communications Technology Security Manual, ACSI 33 (19 September 2005)
Defence Signals Directorate
<http://www.dsd.gov.au/library/infosec/acsi33.html>
3. ICT Security Policy for the Use of BlackBerry by the Australian Government (July 2005)
Defence Signals Directorate
http://www.dsd.gov.au/lib/pdf_doc/library/BlackBerry_Policy_July05.pdf
4. BlackBerry Guidance
Australian Government Information Management Office
 - (a) Instructions on the Allocation and Use of BlackBerry Personal Electronic Devices in Australian Government Agencies (October 2005)
 - (b) Better Practice Guidance 23 – Use of BlackBerry Devices (October 2005)
 - (c) Better Practice Guidance 24 – User Requirements for BlackBerry Devices (October 2005)
<http://www.agimo.gov.au>
5. Australian Government Metadata Standard for Electronic Mail
<http://naa.gov.au>
6. Email Protective Marking Standard for the Australian Government – Version 1 – (October 2005)
<http://www.agimo.gov>
7. Internet Message Format, RFC 2822, April 2001
<http://www.ietf.org/rfc/rfc2822>
8. Enhanced Security Services for S/MIME. RFC 2634, June 1999
<http://www.ietf.org/rfc/rfc2634.txt>

Document Revision History

Version	Date	Comments
0.85	20 July 2005	Initial exposure draft. (Protective Marking Working Group, CIOC, IIWG, SIG)
0.9	5 August 2005	Added summary server behaviour actions (Section 6.1.5) Updated email blocking and logging (Section 6.4) Updated sample email rejected messages (Appendix B) Completed sections 2, 3, 4, Appendix A Added Glossary of Terms (Appendix C) Feedback incorporated as appropriate Editorial changes
1.0	1 October 2005	General minor revisions based on release of PSM 2005 and ACSI 33 (19 September 2005) Added PSM, ACSI 33 compliance statement. Sections 1.2, 6.4 updated based on revised ACSI 33. Inserted new section 4.1 to reflect 'no default' setting for protective marks in email client tools.

1 Introduction

Email communications are a widely used and an accepted form of official business communication by and within the Australian Government. As such, they provide essential evidence of the conduct of Government business, and are important information assets of the Australian Government. Formal government communications such as emails should be controlled by standardised business processes and within information management regimes that protect the interests of citizens and the Commonwealth in a cost efficient manner.

Standardising the metadata for transmission with emails will facilitate corporate control and efficient processing and management of these important records for business purposes. It will enable automated processing of the distribution and control of emails, and the capture of important information about the business context of the communications with the emails themselves into the information systems of government agencies. Additionally, assigning standardised metadata to business emails at the point of creation will facilitate the capture of these emails into agency systems designed to manage records.

The Commonwealth Protective Security Manual (PSM) [1] states that information requiring a protective marking but held on IT systems should be identified in the same or equivalent way as information held on another medium and given the same level of protection. ACSI 33 [2] further defines that agencies must ensure that all agency-originated emails that contain security classified information are marked with a protective marking that identifies the maximum classification for that information.

In the context of the Australian Government MetaData Standard for Electronic Mail [5] and within the policy requirements of the PSM and ACSI 33, this document provides detailed implementation guidance for agencies on the inclusion of protective markings for email. It describes the email client requirements, user guidelines and the server behaviour rules that must be considered in implementing the new requirements of ACSI 33. This guide will assist agencies working to implement protective markings quickly, and in a manner that is consistent with the email metadata standard.

The relationship between the policy and various standards documents is shown in Figure 1.

The implementation of a subset of the metadata standard addressing the need to include protective security markings in email will allow Australian Government agencies to:

- attach appropriate protective markings to email, and associated attachments at the desktop;
- recognise and deal with these markings at the email server gateways, including when sending email to and from mobile wireless devices, such as BlackBerry; and
- enable appropriate security management of email records in both business systems and dedicated recordkeeping systems.

This will assist in controlling the inappropriate transmission of information across network paths not classified to carry such information, and to ICT systems not secured to store and process classified information.

This implementation guide should be read in conjunction with ACSI 33, the “Email Protective Marking Standard for the Australian Government” and the DSD’s “ICT Security Policy for the use of BlackBerry”.

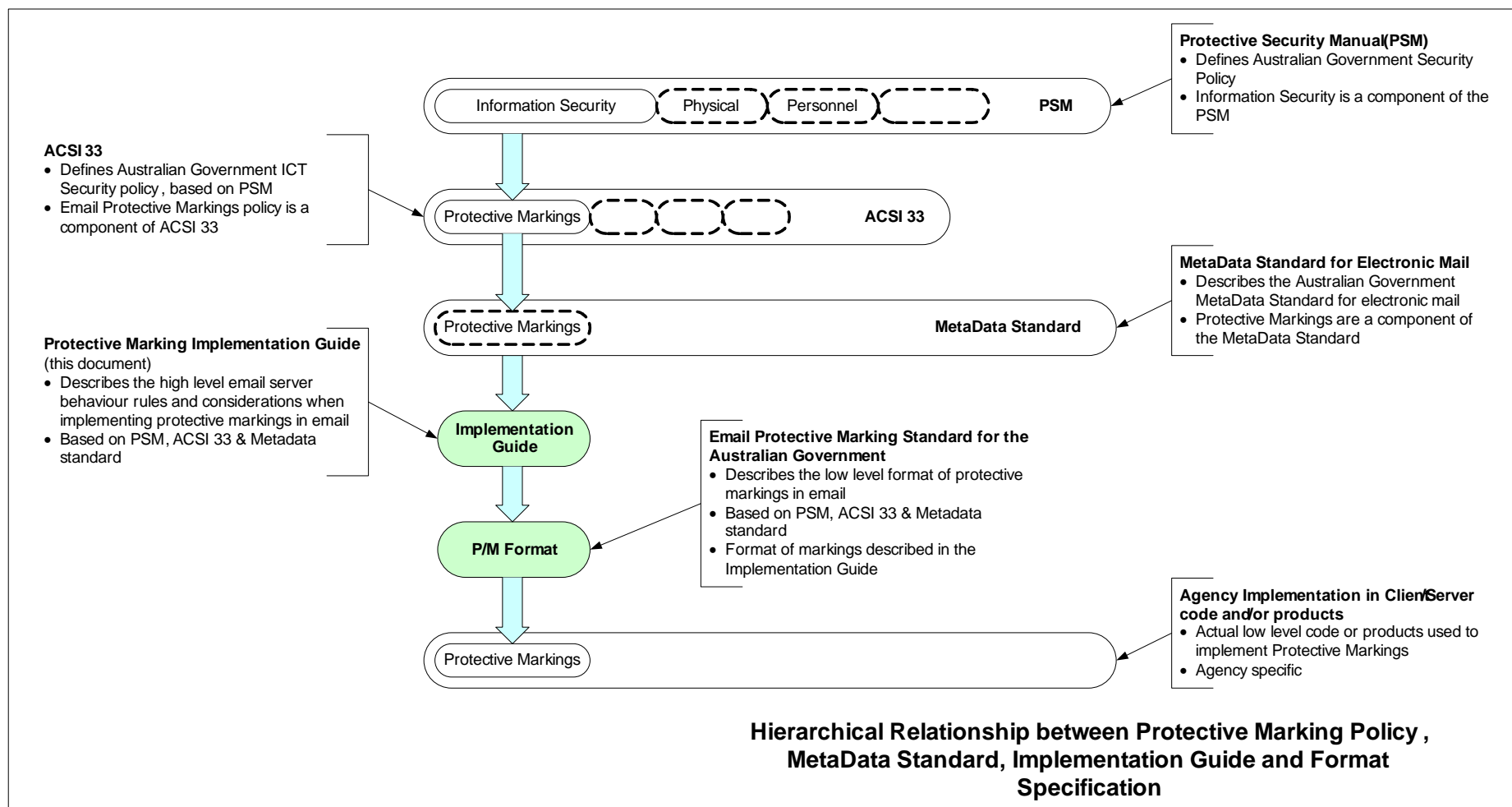


Figure 1 - Relationship between national policy, email protective marking policy, metadata standard and implementation guide

1.1 Scope

The scope of this Implementation Guide is: the inclusion of protective markings in email; and the attached protective marking to be plainly visible to the user.¹ It is intended as a consistent whole of government guide for agencies to be able to quickly implement the requirement for protective markings in email prescribed in the March 2005 release of ACSI 33.

This document provides guidance on:

- User awareness and email policy considerations;
- Email client functionality including for remote, mobile and portable devices;
- Email server considerations and behaviour for inbound / outbound and forwarded email; and
- Rejected email behaviour.

The format of the protective markings is described in the “Email Protective Marking Standard for the Australian Government” [6].

In implementing protective markings in email, this guide does not address:

- Individual agency policy decisions, associated waivers and their impact;
- Physical security considerations;
- Encrypted email and encrypted email attachments;
- The protective marking or labelling of other formatted data e.g. FTP data transfers across FedLink, private network links or the internet;
- Instant messaging, SMS text messaging etc.²; and
- Whether the individual’s clearance level is appropriate to the classification of the material sent or received.

This guide makes particular reference to BlackBerry devices. However, the controls described should be seen in the more general context of protective markings for all email irrespective of the method of delivery or access. Further considerations for remote and mobile access to email are discussed in Section 8.

Each agency will need to analyse their respective email architecture, implementation and business requirements and assess the considerations described in this guide within their particular environments.

1.2 Timing

DSD recommends that agencies maintain compliance with the latest release of ACSI 33. However, it recognises that it takes time to implement new or revised security controls. To accommodate this issue, the policy allows an agency to be compliant with any release of the manual as long as it is no more than two years old. This means

¹ This means that protective markings must be included in an email’s ‘Subject:’ line and mail headers. See Section 2.

² AGIMO will consult with agencies and DSD as the Australian Government policy and business requirements for these services mature.

that all Australian Government Agencies must have implemented and be using protective markings in email by March 2007.

Agency's failing to meet these standards by March 2007 must have an endorsed waiver in place as described in Part A of the PSM. However, where a proposed waiver could impact upon the protection provided to information of another Australian Government agency, those agency's must be consulted before the waiver is granted.

The considerations relating to the staggered implementation of protective markings in email by Australian Government agencies are further discussed Section 6.8.

1.3 Implementation Path

Protective markings are a subset of the Australian Government email metadata standard. It is envisaged that the inclusion of protective markings in email is the first of a number of stages in implementing the full metadata standard. The implementation path may be viewed as:

1. Development of an Implementation Guide for the client/server behavioural rules in implementing protective markings;
2. Development of a protective marking format standard;
3. Specification development of an email client 'plug-in' supporting the metadata standard;
4. Implementation of the full metadata standard across Australian Government agencies; and
5. Address the updated functionality requirements of email clients (e.g. Outlook, Lotus Notes, web browsers, BlackBerry) to support the metadata standard.

These broad activities may be undertaken concurrently, as appropriate, dependent on available resource or priority.

From an agency perspective the implementation of protective markings may be further divided into a number of phases, e.g.:

- Development of an email client plug-in to facilitate the addition and display of protective markings;
- Undertake user awareness and training;
- Implementation of the outbound behaviour rules at the identified email gateways;
- Identify and modify server generated emails;
- Implement inbound rules on an agency-by-agency agreement basis;
- Implement inbound server behaviour rules for all FedLink connections; and
- Fully implement inbound rules.

In developing and deploying these products and services it is important that there is a consistent implementation across the whole of Government to provide assurance that security classified email only flows to appropriate locations and/or devices. This whole of Government implementation will only be as effective as 'the weakest link in the chain'.

1.4 Intended Audience

This guide is intended for information technology professionals involved in the planning, architecture, design, development, configuration or administration of an agency's email infrastructure. Because of the nature of the problem to be addressed, this document contains an amount of technical material.

It is generally useful for:

- Business managers wishing to understand the impact of including protective markings in email and the required controls over the flow of security classified material;
- Agency security advisers (ITSA, ASA) in implementing the requirements of ACSI 33 and the PSM;
- Policy makers involved in developing an agency's email policy;
- Records managers wishing to understand the implications of implementing the Australian Government metadata standard; and
- IT support staff involved in developing user awareness and staff induction material or in the provision of user support services.

1.5 Assumptions

In developing this guide the following assumptions have been made:

- As there is no defined Australian Government standard for personal or unofficial emails, the protective marking of UNCLASSIFIED has been used to include this category. Server behaviour rules may be easily modified to include an additional protective marking if defined;
- The protective marking displayed on an email reflects the highest classification of material contained in that email; and
- Agency staff are trained in protective security and classification requirements.

1.6 Protective Marking Implementation Discussion Forum

A web based protective marking discussion forum has been created by the Australian Bureau of Statistics and is available at:

<http://forums.abs.gov.au/registration/EmailForum>

1.7 Contacts

This guide draws on information from many sources. Advice on specific areas should be directed to the appropriate agency:

- Commonwealth protective security policy.
Attorney-General's Department
Protective Security Coordination Centre
Email: psm@ag.gov.au
Phone 02 6250 6666
URL: <http://www.ag.gov.au>
- Protective security policy and procedures in communications and information technology.
Defence Signals Directorate
Email assist@dsd.gov.au
Phone 02 6265 0197
Fax 02 6265 0328
URL <http://www.dsd.gov.au>
- Australian Government Metadata Standard for Electronic Mail
National Archives of Australia
Digital Government Recordkeeping Helpline
Email: recordkeeping@naa.gov.au
Phone: 02 6212 3610
URL: <http://naa.gov.au>
- Implementation Guide for Email Protective Markings and the Email Protective Markings Standard
Australian Government Information Management Office
Emerging Technologies Team
Email: better.practice@finance.gov.au
Phone: 02 6215 1546
URL: <http://www.agimo.gov.au/practice/delivery/checklists>

2 Background

This section provides some very brief background introductory material to internet email and the ‘headers’ included in an email message.

2.1 Email Headers

Email messages are composed of two parts: a header followed by the body. The body of an email may contain virtually anything.³ The header contains lines of information that must strictly conform to certain standards. This is shown in Figure 2.

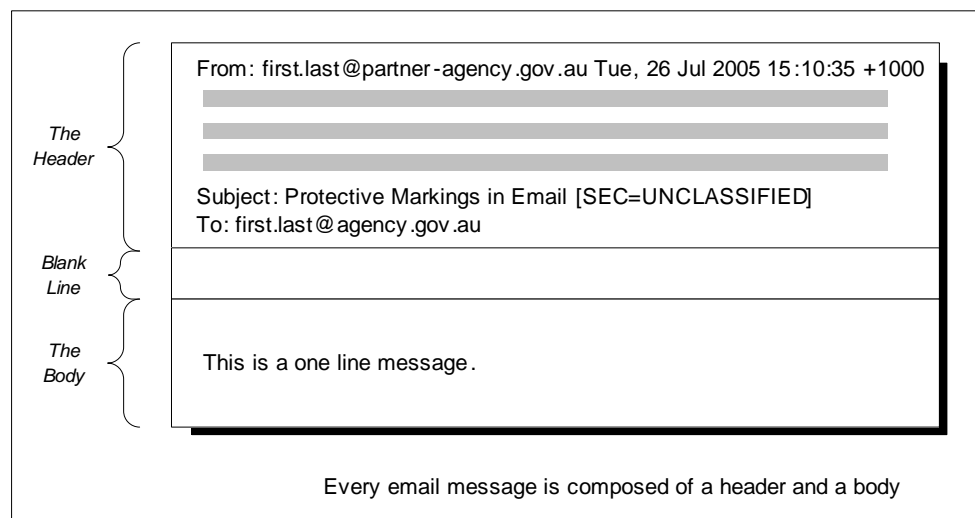


Figure 2 - Email headers and message body

Most header lines start with a word followed by a colon. Each word tells what kind of information the rest of the line contains. There are many types of header lines that can appear in a mail message. Some are mandatory, some are optional, and some may appear many times. A complete list of header lines may be found in RFC 2822 [7].

2.2 Protective Marking Standard for Email

The “Email Protective Marking Standard for the Australian Government” [6] defines the format of protective markings that may be included in internet email messages exchanged between Australian Government agencies. The protective marking is used to convey the security classification of information in a message, as defined within PSM.

The Standard defines two ways in which the PSM protective markings can be applied to email messages:

1. Appending the marking to the ‘*Subject:*’ email header line using a specified syntax; and
2. Including the marking in an Internet Message Header Extension using a specified syntax.

³ With the advent of MIME (Multipurpose Internet Mail Extensions), the message body can now be composed of many mini-messages, each with its own MIME header and sub-body.

These are basic syntaxes and so should be easy to implement in sending and receiving email agents. A more advanced method (and hence more difficult to implement) is available where the protective marking is conveyed in a digitally signed S/MIME security label [8]. This method is considered out of scope for the current activity.

The protective marking must be included as part of the '*Subject:*' line. If it is only included as part of the email headers it will not be visible to all recipients unless they have a modified email client that is capable of displaying this extra information. This is particularly so for portable wireless devices including BlackBerry. The requirement to include the protective marking in the emails '*Subject:*' line may diminish over time.

Research in Motion (RIM, the BlackBerry supplier) has also advised that all email headers except for the '*To:*', '*From:*' and '*Subject:*' lines are stripped from messages transferred to BlackBerry devices. This means that if the protective marking is only included as part of the email's header, it will be removed when it is transmitted to the BlackBerry device.

3 Email Policy and User Awareness Guidelines

The Commonwealth Protective Security Manual states that information requiring a protective marking but held on IT systems should be identified in the same or equivalent way as information held on another medium and given the same level of protection. ACSI 33 further defines that agencies must ensure that all agency-originated emails that contain security classified information are marked with a protective marking that identifies the maximum classification for that information.

Agencies should review their email policy, user or internet usage guidelines and ensure that they address the requirement for the inclusion of protective markings using the syntax described in the protective marking standard [6].

As agencies have developed their policies and procedures using different methods, templates, and with varying agency business requirements and will use different software tools or methods to include protective markings, this section lists a number of topics that should be addressed by an agency's email documentation.

Policy and usage guidelines should include information on:

- Policy requirement for the inclusion of protective markings in email;
- Scope of requirement to include protective marking (e.g. original messages, replies, forwards, out-of-office auto replies);
- How to classify an email and any attachments;
- The format and location of the protective marking;
- The implications of over or under classification of information;
- The classification of email that may be transmitted on an agency's internal network;
- Sending security classified information to external addresses over the internet;
- The classification of information that may be transmitted to a FedLink connected agency;
- How to find out what classification of information another agency will accept;
- The classification of information that may be transmitted to/from a BlackBerry or any wireless connected device;
- What will happen if you attempt to send a message that exceeds the security rating of the recipient's system;
- Why an email may be rejected;
- What to do if you receive a 'rejected email' message;
- Whether the sender or recipient of a 'rejected' email is notified;
- Whether 'rejected' emails are logged or delivered;
- What to do if you receive a message without a protective marking;
- What to do when forwarding an email that does not contain a protective marking to another user;
- Whether your agency has implemented a 'default' protective marking for email; and
- How to classify 'personal' emails.

Example user guidelines are contained at Appendix A.

4 Email Clients ⁴

Implementing protective markings in email may be achieved by: ⁵

- the user manually typing the marking into an email's '*Subject:*' line;
- using a 3rd party or in-house developed software 'plug-in' or 'drop-down' box in the email client to include the protective marking in the '*Subject:*' line and email header; or
- having the facilities natively embedded into the email client by the vendor.

It is envisioned that native vendor support for protective markings and the full metadata standard may take some time to negotiate and implement. As such, the first two methods are the most likely to be implemented in the short to medium term.

Email client support for the inclusion of protective markings should be implemented for all email clients in use across the agency. This may include e.g. Microsoft Outlook, Lotus Notes, various web browsers, and handheld and portable devices (PDAs) including BlackBerry.

4.1 'No Default' Protective Marking

As defined in ACSI 33 user-generated emails should not be configured with an agency wide 'default' marking. Additionally, email clients should only present the user with a list of protective markings for which the agency's ICT systems are accredited.

E.g. If an agency is accredited to store and process up to X-IN-CONFIDENCE material, the email tool should be configured to only present UNCLASSIFIED and X-IN-CONFIDENCE protective marking choices to the user.

4.2 3rd Party Products

Table 1 lists a number of 3rd party email client 'plug-ins' and content filtering ⁶ products in use across Australian Government agencies. This is not an exhaustive list. They are provided for reference only as tools that may or may not be helpful in implementing and managing protective markings in email. They in no way imply any form of endorsement for the respective products or services.

⁴ Mail User Agents (MUA).

⁵ The resultant protective marking must be clearly visible to the intended recipient of the email.

⁶ Content filtering products may be used to implement the server behaviour rules discussed in Section 6.1.

Product	Category	Platform	Web Reference
janusSEAL	<ul style="list-style-type: none"> Email client 	<ul style="list-style-type: none"> Microsoft Outlook Web mail 	www.janus.net.au
MailGate	<ul style="list-style-type: none"> Content filtering 		http://www.tumbleweed.com/products/mailgate/index.html
Mail Marshall	<ul style="list-style-type: none"> Content filtering 	<ul style="list-style-type: none"> Microsoft Exchange 	http://www.essential.co.uk/Products/MailMarshal.asp
MIMESweeper SMTP MIMESweeper for Exchange	<ul style="list-style-type: none"> Content filtering 		www.clearswift.com
SafeSend SecureAge Trex	<ul style="list-style-type: none"> Email client S/MIME Content filtering 	<ul style="list-style-type: none"> Microsoft Outlook Lotus Notes Web mail 	http://www.eb2b.com.au/index_solutions.htm
Titus	<ul style="list-style-type: none"> Email client 	<ul style="list-style-type: none"> Microsoft Outlook 	http://www.titus-labs.com/software/index.html

Table 1 - 3rd Party email client and content filtering products

A number of agencies have also developed their own email ‘plug-in’ solutions for Lotus Notes and Microsoft Outlook, embedding the protective marking in the ‘*Subject:*’ line and email header.

5 Email Architecture

This section provides a reference two layer logical email architecture (see below). It is used to analyse and illustrate the flow of email from one location to another, highlighting the entry and exit points, into and out of an agency. As there are many ways to design and deploy networks, and various email filtering mechanisms in place across the Australian Government, agencies should analyse their respective environments to identify all email flows. Having identified these flows and the entry and exit points for email in the agency environment, behaviour rules may be implemented to protect the transmission of classified information consistent with policy.

Figure 3 illustrates the high level flow of email between an agency and its business partners. It also shows the various mechanisms used to remotely access email, including BlackBerry.

Figure 4 shows a more detailed analysis of the logical reference email architecture depicting a typical two layer environment. It shows an:

- email gateway environment which relays email from outside servers to the internal email servers and vice versa; and
- internal email environment that routes intra-organisation email, sends outbound email to the external server, and allows internal users to access email.

It also shows the placement of the BlackBerry Enterprise Server (BES) used for receiving and forwarding email to BlackBerry devices via the Research in Motion (RIM) environment.

The purpose of analysing email flows and the architecture of the email system is to identify where in the environment, controls or filtering rules need to be implemented.

This reference model is used through this document to illustrate the issues that agencies should consider in implementing protective markings for email.

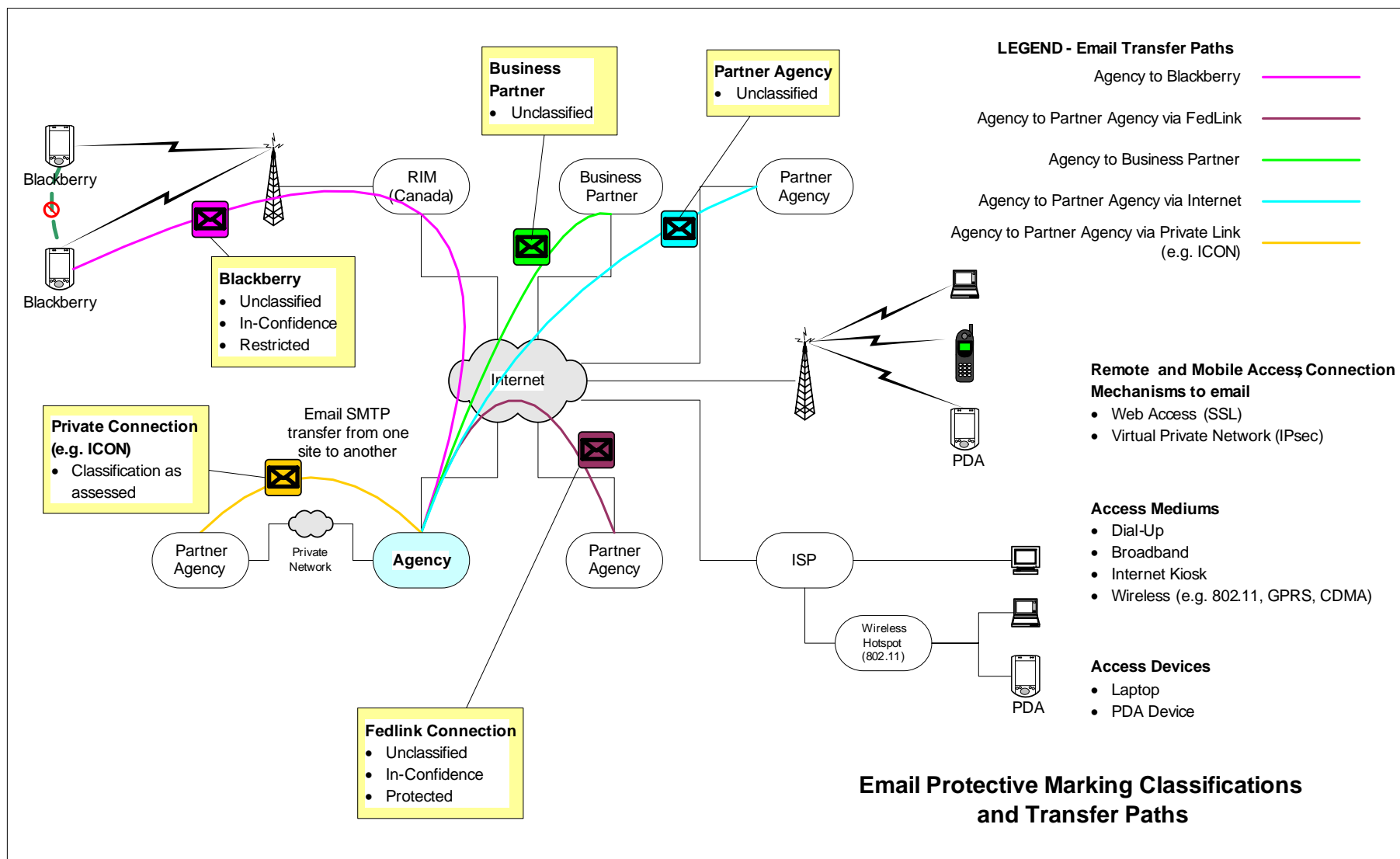


Figure 3 - High level email transmission paths

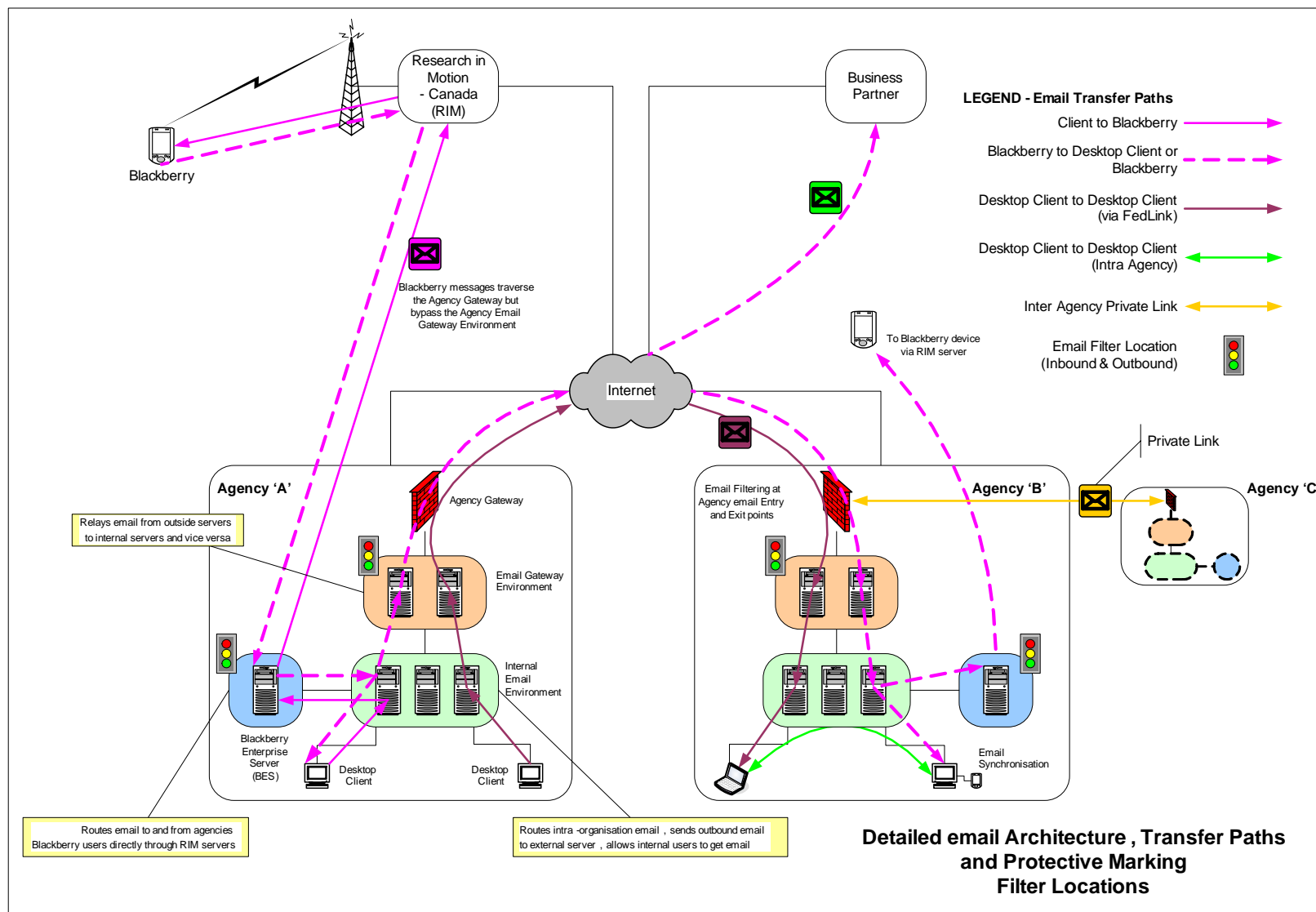


Figure 4 - Detailed email architecture

6 Email Server Considerations

This section discusses the implementation considerations for the filtering of emails based on their security classification as shown by their protective marking at the identified email entry and exit servers based on the reference model (Section 5).

6.1 Server Behaviour Rules

To support the protective marking standards defined in ACSI 33, controls must be implemented at the identified email servers. This section provides an example of the server processing behaviour using the reference email architecture. Agencies should verify and implement rules based on their own particular environmental analysis.

It is important that there is a consistent implementation of these server rules across the whole of Government to provide assurance that security classified email only flows to appropriate locations and/or devices.

The underlying principles used in developing these rules include:

- The general security principles of:
 - “that which is not expressly permitted is denied”; and
 - “defence-in-depth”.
- Filtering must occur for outgoing, incoming and forwarding of email;
- X-IN-CONFIDENCE does not include CABINET-IN-CONFIDENCE;
- Precedence, or the order in which rules are processed should be considered; and
- BlackBerry is treated as an extension of an agency’s internal network.

The actions to be undertaken on email not meeting the defined rules are discussed in Section 6.4 and 6.6.

6.1.1 Email Originating from Outside of the Australian Government

External organisations are not bound by the Australian Government requirements of the PSM or ACSI 33. ACSI 33 recommends that these organisations be encouraged to adopt the protective marking system. However, it is highly likely that agencies will receive email from individuals or external organisations without a protective marking.

Agencies should refer to ACSI 33 and decide how they will deal with emails from outside of the Australian Government. This is important in considering the server behaviour of inbound and forwarding of email.⁷

An alternative to the automatic addition of a ‘gateway’ generated default marking may be for the email client to display a message to inform the user that the information has not had a protective marking applied. ACSI33 suggests:

“Note: This email was not from an Australian Government source and has been automatically marked as UNCLASSIFIED.”.

This informs the user that the email has been received without a protective marking. If

⁷ In analysing the email flows there appear to be advantages in following the RECOMMENDED practice described in ACSI 33.

the user then replies or forwards the email they will need to apply a protective marking.

Section 6.8 provides additional information for the processing of inbound email from Australian Government agencies as they deploy their respective solutions.

6.1.2 Outbound email (sending)

ACSI 33 specifies that agencies must ensure that all agency-originated emails that contain security classified information are marked with a protective marking. This section describes the outgoing server behaviour rules based on the reference model.

It should be noted that 'outgoing email' includes, but is not limited to:

- manual and automatic 'forwarding' of email;
- original messages;
- meeting requests; and
- 'out-of-office' replies.

Whether an email is outbound or inbound is dependent on the reference point. E.g. an email may be outbound from one agency, then seen as inbound at the recipient agency, and may again be outbound from that recipient agency, if it is on-forwarded to e.g. a BlackBerry device. The appropriate rule set (inbound or outbound) should be applied at the appropriate interface.

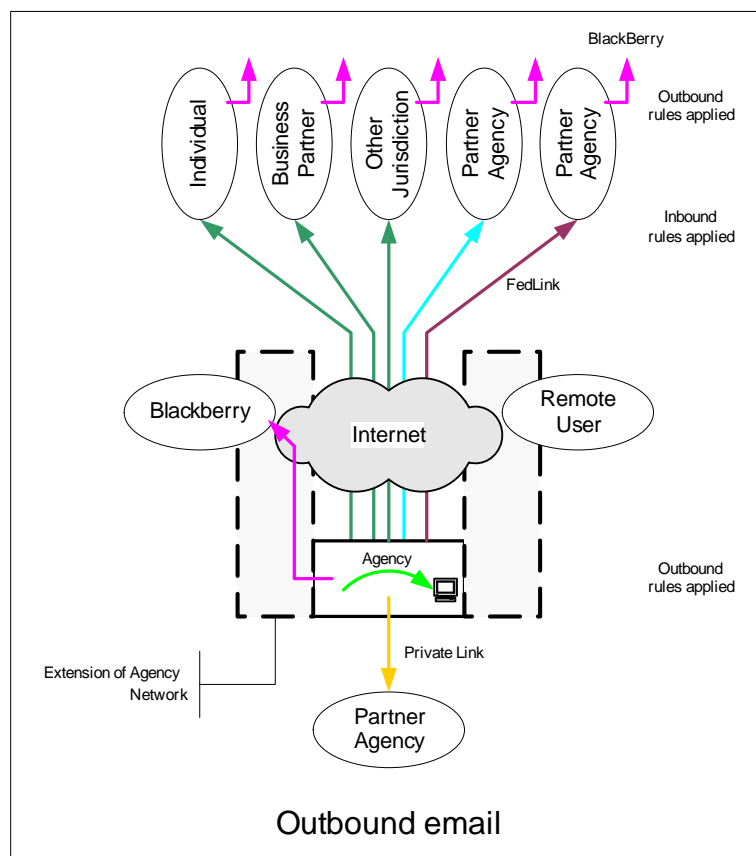


Figure 5 - Outbound email

Figure 5 illustrates agency outgoing email paths. The following tables should be read with reference to this diagram.

Table 2 summarises the defined permitted protective markings based on the receiving system and the path over which the email is transferred. This summary table is further developed into the server behaviour rules in

Table 3. It should be noted that the server behaviour rules must be applied for every valid agency email address in the To:, Cc: and Bcc: header lines and across multiple domains (agency and business partners).

Outbound To	ACSI 33 (or FedLink) Defined Permitted Classification ⁸
Agency (Intra-agency)	Appropriate to agency network classification
BlackBerry (Intra-agency)	UNCLASSIFIED ⁹ IN-CONFIDENCE RESTRICTED
Partner Agency (Inter-agency - Private Link)	Appropriate to private network classification
Partner Agency (Inter-agency - FedLink connected)	UNCLASSIFIED ¹⁰ IN-CONFIDENCE PROTECTED
Partner Agency (Inter-agency - unprotected public network connected e.g. internet)	UNCLASSIFIED
Business Partner (unprotected public network connected)	UNCLASSIFIED
Business Partner (encrypted across public network)	Appropriate to ACSI 33 cryptographic requirements and approved cryptographic protocols (DACPs) ¹¹

⁸ Agency policy may define more restrictive controls e.g. an agency may only permit UNCLASSIFIED material to a BlackBerry device or over FedLink. Server behaviour rules may be adjusted according to agency policy.

⁹ Assumes device is compliant with “ICT Security Policy for the Use of BlackBerry by the Australian Government” [3] i.e. uses version 3.6 to 4.x of BlackBerry software.

¹⁰ These classification levels are permitted over FedLink. However, some agency’s only connect to FedLink at the IN-CONFIDENCE level, so information classified PROTECTED must not be transmitted to these agency’s. Refer to the FedLink members’ Web site.

¹¹ DACP – DSD Approved Cryptographic Protocols
Added for completeness only, but out of scope for this document

Table 2- Outbound email, defined permitted security classifications

Outbound To	Email Traverses	Filter Rule (on send)	Filter Location(s)
Internal to Internal ¹² (Intra agency)	<ul style="list-style-type: none"> • Internal Email Environment 	Permit if: <ul style="list-style-type: none"> • Classification appropriate to agency network classification 	<ul style="list-style-type: none"> • Internal Email Environment
Internal to BlackBerry (Intra agency – extension of agency network)	<ul style="list-style-type: none"> • Internal Email Environment • Agency BES • Internet • RIM • Wireless network 	Permit if: <ul style="list-style-type: none"> • Classification appropriate to agency network classification; AND • Classification == UNCLASSIFIED, IN-CONFIDENCE or RESTRICTED 	<ul style="list-style-type: none"> • Internal Email Environment • Agency BES
Internal to Private connection (Inter agency – e.g. ICON)	<ul style="list-style-type: none"> • Internal Email Environment • Email Gateway Environment • Agency Gateway • Private Network • Destination Partner Environment 	Permit if: <ul style="list-style-type: none"> • Classification appropriate to agency network classification; AND • Email classification is appropriate to the classification of the private link ¹³ 	<ul style="list-style-type: none"> • Internal Email Environment • Email Gateway Environment
Internal to FedLink connected agency	<ul style="list-style-type: none"> • Internal Email Environment • Email Gateway Environment 	Permit if: <ul style="list-style-type: none"> • Classification appropriate to 	<ul style="list-style-type: none"> • Internal Email Environment

¹² Assumes internal email environment email server to email server communication links are secured appropriately.

¹³ Requires agency private link 'lookup table' (see Section 6.3)

¹⁴ Requires FedLink lookup table (see Section 6.2)

Outbound To	Email Traverses	Filter Rule (on send)	Filter Location(s)
(Inter agency)	<ul style="list-style-type: none"> • Agency Gateway • FedLink • Destination Agency Gateway 	agency network classification; AND <ul style="list-style-type: none"> • Classification == UNCLASSIFIED, IN-CONFIDENCE or PROTECTED; AND <ul style="list-style-type: none"> • Destination agency can receive this classification via FedLink ¹⁴ 	<ul style="list-style-type: none"> • Email Gateway Environment
Internal to Partner Agency across unprotected public network (Inter agency - e.g. another jurisdiction)	<ul style="list-style-type: none"> • Internal Email Environment • Email Gateway Environment • Agency Gateway • Internet • Destination Partner Environment 	Permit if: <ul style="list-style-type: none"> • Classification == UNCLASSIFIED 	<ul style="list-style-type: none"> • Internal Email Environment • Email Gateway Environment
Internal to Business Partner across unprotected public network (Inter organisation or individual)	<ul style="list-style-type: none"> • Internal Email Environment • Email Gateway Environment • Agency Gateway • Internet • Destination commercial partner environment 	Permit if: <ul style="list-style-type: none"> • Classification == UNCLASSIFIED 	<ul style="list-style-type: none"> • Internal Email Environment • Email Gateway Environment

Table 3 - Outbound email server rules

6.1.3 Inbound email (receiving)

This section describes the filtering actions for inbound email. As noted in Section 6.1.2, whether an email is inbound or outbound is dependent on the reference point. E.g. An email may be incoming from one agency, if it is then on-forwarded or transmitted to a BlackBerry device it is then seen as outgoing from the agency. The appropriate rule set (inbound, outbound or forwarding) should be applied at the appropriate interface.

In essence the server rules for inbound email are simpler than for outgoing email as an agency has little or no control over what they receive. However, if the email is received from an Australian Government agency the policies and standards prescribed by the Protective Security Manual (PSM) and ACSI 33 that define the requirements for adding and filtering on protective markings apply.

Table 4 summarises the defined permitted protective markings based on the receiving system and the path over which the email is transferred. This summary table is further developed into the server behaviour rules in Table 5.

The server behaviour rules for inbound email originating from non Australian Government agencies must cater for emails with anything or nothing in the ‘*Subject:*’ header (See Section 6.1.1).

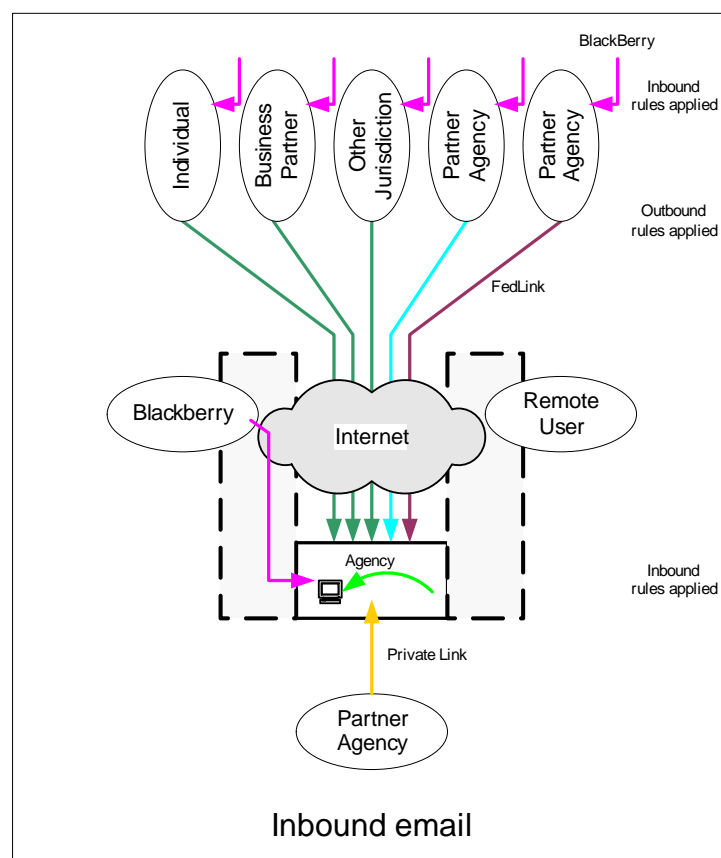


Figure 6 - Inbound email

Inbound From	ACSI 33 (or FedLink) Defined Permitted Classification¹⁵
Agency (Intra-agency)	Appropriate to agency network classification
BlackBerry (Intra-agency)	UNCLASSIFIED ¹⁶ IN-CONFIDENCE RESTRICTED
Partner Agency (Inter-agency - Private Link)	Appropriate to private network classification
Partner Agency (Inter-agency - FedLink connected)	UNCLASSIFIED ¹⁷ IN-CONFIDENCE PROTECTED
Partner agency (Inter-agency - unprotected public network connected e.g. internet)	UNCLASSIFIED
Partner agency (Inter-agency - Other jurisdictions across unprotected public network e.g. internet)	Any or no Protective Marking
Business Partner or individual (Inter-organisation across unprotected public network e.g. internet)	Any or no Protective Marking
Business Partner (encrypted across public network e.g. internet)	Appropriate to ACSI 33 cryptographic requirements and approved cryptographic protocols (DACPs) ¹⁸

Table 4 - Inbound email, defined permitted security classifications

¹⁵ Agency policy may define more restrictive controls e.g. an agency may only permit UNCLASSIFIED material to a BlackBerry device or over FedLink. Server behaviour rules may be adjusted according to agency policy.

¹⁶ Assumes device is compliant with "ICT Security Policy for the Use of BlackBerry by the Australian Government", July 2005 [3] i.e. uses version 3.6 to 4.x of BlackBerry software.

¹⁷ These classification levels are permitted over FedLink. However, some agency's only connect to FedLink at the IN-CONFIDENCE level, so information classified PROTECTED must not be transmitted/received to/from these agency's. Refer to the FedLink members Web site.

¹⁸ DACP – DSD Approved Cryptographic Protocols
Added for completeness only, but out of scope for this document

Inbound From	Traverses	Filter Rule (on receipt)	Filter Location(s)
Internal to Internal ¹⁹ (Intra agency)	<ul style="list-style-type: none"> Internal Email Environment 	Permit if: <ul style="list-style-type: none"> Classification appropriate to agency network classification 	<ul style="list-style-type: none"> Internal Email Environment
Agency BlackBerry (Intra agency - extension of agency network)	<ul style="list-style-type: none"> Wireless network RIM Internet Agency BES Internal Email Environment 	Permit if: <ul style="list-style-type: none"> Classification == UNCLASSIFIED, IN-CONFIDENCE or RESTRICTED; AND Classification appropriate to agency network classification 	<ul style="list-style-type: none"> Agency BES Internal Email Environment
Private network connection (Inter agency - e.g. ICON)	<ul style="list-style-type: none"> Agency Gateway Email Gateway Environment Internal Email Environment 	Permit if: <ul style="list-style-type: none"> Email classification is appropriate to the classification of the private network ²⁰; AND Classification appropriate to agency network classification 	<ul style="list-style-type: none"> Email Gateway Environment

¹⁹ Assumes internal email environment email server to email server communication links are secured appropriately.

²⁰ Requires agency private link 'lookup table' (see Section 6.3)

Inbound From	Traverses	Filter Rule (on receipt)	Filter Location(s)
Partner agency (Inter agency - FedLink connected)	<ul style="list-style-type: none"> FedLink Agency Gateway Email Gateway Environment Internal Email Environment 	Permit if: <ul style="list-style-type: none"> Classification == UNCLASSIFIED, IN-CONFIDENCE or PROTECTED; AND Agency can receive this classification via FedLink ²¹ 	<ul style="list-style-type: none"> Agency Email Gateway Environment
Partner agency (Inter agency - unprotected public network connected e.g. internet)	<ul style="list-style-type: none"> Internet Agency Gateway Email Gateway Environment Internal Email Environment 	Permit if: <ul style="list-style-type: none"> Classification == UNCLASSIFIED ^{22 23} 	<ul style="list-style-type: none"> Email Gateway Environment
Partner agency (Inter agency - other jurisdictions, unprotected public network connected e.g. internet)	<ul style="list-style-type: none"> Internet Agency Gateway Email Gateway Environment Internal Email Environment 	Permit all: <ul style="list-style-type: none"> i.e. with or without a protective marking on the email ²⁴ 	<ul style="list-style-type: none"> Email Gateway Environment
Business Partner or Individual (Inter organisation - unprotected)	<ul style="list-style-type: none"> Internet Agency Gateway Email Gateway Environment 	Permit all: <ul style="list-style-type: none"> i.e. with or without a protective marking on the email 	<ul style="list-style-type: none"> Email Gateway Environment

²¹ Requires FedLink lookup table (see Section 6.2)

²² Reject if: Classification == IN-CONFIDENCE, RESTRICTED, PROTECTED, HIGHLY PROTECTED, RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET

²³ See also Section 6.8

²⁴ See also Section 6.1.1

Inbound From	Traverses	Filter Rule (on receipt)	Filter Location(s)
public network connected e.g. internet)	<ul style="list-style-type: none"> Internal Email Environment 		

Table 5 - Inbound email server rules

6.1.4 Forwarding email (receive and send)

The rules outlined in Sections 6.1.2 and 6.1.3 generally cover the forwarding of email, i.e. where an email is received (inbound rules) and then sent (outbound rules) to another individual or group. However, there is a special case where an email is received from a non Australian Government agency, without a protective marking, which is then either automatically forwarded to a BlackBerry device, via the internal email environment, or manually on-forwarded by the recipient.

As noted in Section 6.1.1, agencies should decide how they will deal with emails from outside of the Australian Government. This decision will define the server behaviour rules in the following scenarios.

6.1.4.1 Auto Forwarding of email to BlackBerry Device

The implementation must cater for email received (inbound) from an external organisation or individual with no protective marking, where that email is then automatically forwarded to a BlackBerry device. This is shown in Figure 7.

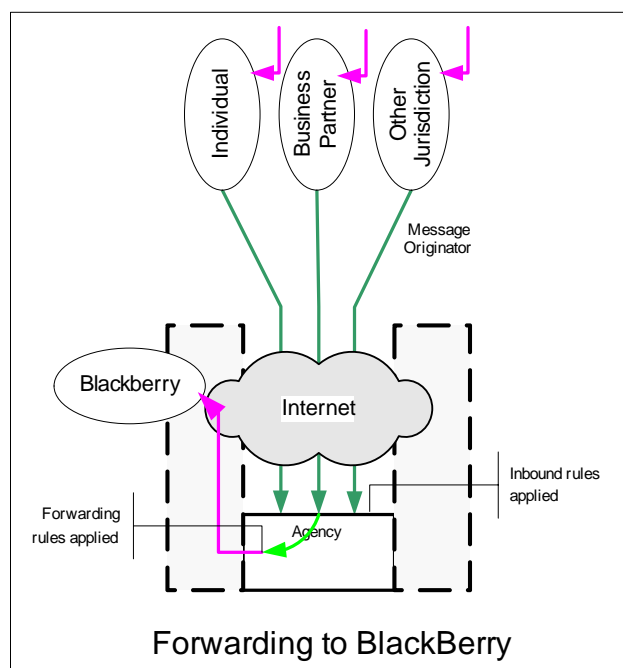


Figure 7 - Auto forwarding of email to BlackBerry device

The email flow and server behaviour are outlined in Table 6.

Message Originator (From:)	<ul style="list-style-type: none"> • Non Australian Government agency or individual
Auto Forwarded To	<ul style="list-style-type: none"> • Agency BlackBerry user
Email Traverses	<ul style="list-style-type: none"> • Internet (inbound) • Agency Email Gateway Environment (inbound) • Agency Internal Email Environment (inbound) • Agency BES (forward/outbound) • Wireless network (outbound)
Forward rule (FW:)	Permit: <ul style="list-style-type: none"> • All i.e. with or without a protective marking on the email; AND / OR • Email Gateway attached agency defined protective marking (as recommended in ACSI 33) – process using outbound rules
Filter Location	<ul style="list-style-type: none"> • Agency Email Gateway Environment • Agency Internal Email Environment • Agency BES

Table 6 - Email flow, auto forwarding to BlackBerry device

6.1.4.2 Manual Forwarding of email

An email may be received (by an agency user) from an external organisation or individual and then manually (or through email client rules) forwarded either internally or externally. Figure 8 illustrates how an email could be forwarded e.g. internally, to a BlackBerry device, to an external user via a private link or across FedLink, or to another jurisdiction.

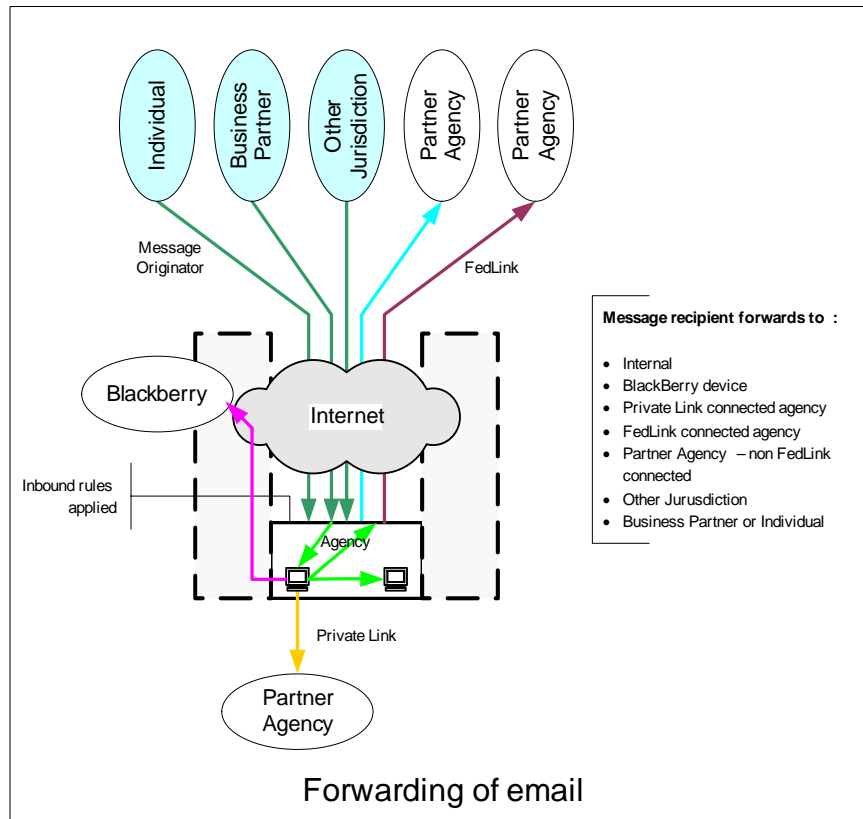


Figure 8 - Recipient forwarding of email

The email flow and server behaviour are outlined in Table 7.

Message Originator (From:)	<ul style="list-style-type: none"> • Non Australian Government agency or individual
Manually Forwarded To	<ul style="list-style-type: none"> • Internal user • Blackberry device • Private link connected user • FedLink connected user • Partner Agency – non FedLink connected • Other jurisdiction – non FedLink connected • Business Partner or individual
Email Traverses	<ul style="list-style-type: none"> • Internet (inbound) • Agency Email Gateway Environment (inbound and forward) • Agency Internal Email Environment (inbound and

	forward) <ul style="list-style-type: none"> • Agency BES (forward) • Private Link (forward) • FedLink (forward)
Forward rule (FW:)	Permit: <ul style="list-style-type: none"> • All i.e. with or without a protective marking on the email; AND / OR • Email Gateway attached agency defined protective marking (as recommended in ACSI 33) – process using outbound rules; OR • Recipient user assigns protective marking on forwarding of email
Filter Location	<ul style="list-style-type: none"> • Agency Email Gateway Environment • Agency Internal Email Environment • Agency BES

Table 7 - Email flow, manual forwarding of email

6.1.5 Summary – Server Behaviour Rules

Table 9 provides a summary of the server behaviour actions described in the preceding sections. The actions of ‘deliver’ and ‘reject’ should also be read in conjunction with the following table (below). The decision to deliver or reject an email is not only based on the classification of the email, and whether it is incoming or outgoing, but also the security rating of the email transfer route.

	Note	Email transfer route
Intra agency email	1	Agency internal network
	2	BlackBerry
Inter agency email	3	Unprotected public network (e.g. internet)
	4	FedLink

Table 8 - Email transfer route key (used in Table 9)

This table should be read in conjunction with Table 8.

If email message classification is:	Outbound If message is being delivered to a network whose classification is:			Inbound If recipient (my) agency network classification is:		
	UNCLASSIFIED	IN-CONFIDENCE	PROTECTED	UNCLASSIFIED	IN-CONFIDENCE	PROTECTED
UNCLASSIFIED (Note: 1,2,3,4)	Deliver	Deliver	Deliver	Deliver	Deliver	Deliver
IN-CONFIDENCE (Note: 1,2,4)	Reject	Deliver	Deliver	Reject	Deliver	Deliver
PROTECTED (Note: 1,4)	Reject	Reject	Deliver	Reject	Reject	Deliver
HIGHLY PROTECTED	Reject	Reject	Reject	Reject	Reject	Reject
National Security (RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET)	Reject	Reject	Reject	Reject	Reject	Reject
Not labelled in accordance with Aust. Govt. classification rules ²⁵ (Note: 3)	Reject	Reject	Reject	Deliver	Deliver	Deliver

Table 9 - Summary server behaviour actions (deliver or reject)

²⁵ See also Section 6.8

6.2 FedLink Lookup Table

Agencies sending (outbound) or receiving (inbound) email via FedLink will require a lookup table that matches the domain names with the classification of the material that an agency will accept over FedLink. This information is currently available on the FedLink members' web site. Table 10 shows an example of this table.

Organisation	Domain Suffix	(Max) Classification of Information Accepted over FedLink
AAA	@aaa.gov.au	UNCLASSIFIED
BBB	@bbb.gov.au @bbb-bb.gov.au	UNCLASSIFIED IN-CONFIDENCE
CCC	@ccc.gov.au	PROTECTED

Table 10 - Example FedLink table for outbound and inbound email

The format, classification of this table, method of update and distribution is currently being defined.

6.3 Private Link Lookup Table

Agencies with private network links²⁶ with other partner agencies (as depicted in the reference architecture) may need to develop a 'lookup table', to ensure that only appropriately classified and marked email is transmitted across these links. This approach may be generally applicable if an agency has a more secure environment within their normal environment. E.g. If their network is rated as IN-CONFIDENCE but they also have a small PROTECTED internal enclave.

6.4 Email Blocking and Logging

Agencies must consider what action will be taken if an email fails the server behavioural rules. Table 11 summarises the actions recommended in ACSI 33.

Rule	Notification that email has been blocked sent to:	Log action
Outbound	Sender	Log email blocked for transmission
Inbound	Intended recipient	Log email rejected from entering

Table 11 - Blocked email notification and logging

In developing a rejected email notification policy, an agency may decide that notifications (including Delivery Status Notifications) are never sent 'outwards' as you cannot rely on the 'Sender', 'From' or 'Reply-to' addresses in a message. All

²⁶ E.g. ICON

notifications, irrespective of whether the email message was inbound or outbound are sent to an internal address, i.e. to the sender in the case of outbound, or the recipient in the case of inbound messages. It is then up to the internal user to action the rejected message.

Agencies should also consider the level of detail to be logged, who has access to this information and their individual security clearance, given the decision to block email generally indicates that the content of the email exceeds the accreditation of the recipient system. Logging of the entire email message (headers, body and attachments) may have the unwanted side effect of raising the security classification of the logging system (including how it then needs to be treated, sanitised and subsequently disposed of) thus potentially exceeding the classification of the agency's network.

An analysis of the blocked email logs may be an indication of the further need for user awareness training in email classification or protective security procedures.

Agencies using Network Intrusion Detection Systems (NIDS) may also wish to consider monitoring SMTP streams for protective markings above their network classification.

Appendix B provides sample rejected email messages.

6.5 Gateway Translation

Some agencies have already implemented protective markings in email. However, their implementation may not be consistent with the protective marking standard [6] or the policy requirements of ACSI 33. As an interim measure, these agencies may consider implementing a translation process at the email gateway for outbound and inbound email to ensure the interoperability of Australian Government email systems.

Example translations may include:

- Moving the protective mark from the beginning of the '*Subject:*' line to the end.
- Modifying the wording or formatting of the protective mark (e.g. SEC: UNCLASSIFIED to/from [SEC=UNCLASSIFIED]).
- Copying the protective mark shown in the '*Subject:*' line to the email headers and/or vice versa.

6.6 Error Conditions

Implementations should cater for errors in the protective marking. E.g if the protective marking is incorrect, truncated or for some reason cannot be processed by the server behaviour rules. The resulting action could be as described above in Section 6.4 for blocked email.

One identified condition is in the transmission of email to BlackBerry devices where the email's '*Subject:*' field (containing the protective marking) may be truncated.

Email gateways should ensure that the full protective markings are included in emails forwarded to BlackBerry devices.

6.7 Server Performance and Testing

The protective mark filtering may impose an additional load on an organisation's email and logging systems. Agencies should load test their configurations, monitor system performance and test the implemented server behaviour rules including message logging and rejection.

6.8 Staggered Implementation of Protective Markings

As indicated in Sections 1.2 and 1.3 agencies may adopt a staggered and/or phased approach to the implementation of protective markings in email leading to a complete implementation by 30 March 2007. After this date an approved waiver will be required if an agency decides not to implement these markings. As such, there may be an interim requirement to accept all inbound email across FedLink, and indeed from all Australian Government agencies without protective markings. This could be achieved by extending the FedLink lookup table (Section 6.2) by adding a 'status' field to indicate whether an agency has or has not implemented protective markings or has a waiver in place. If an agency has implemented markings then the server behaviour should be as described in Section 6.1, if not then the agency may decide to accept (inbound) email without a protective marking, while also deciding whether to add a gateway mark as outlined in Section 6.1.1.

Because of this variable schedule agencies will need to register their implementation status for the addition of protective markings. This information will then be appended to the FedLink lookup table to control the flow of email. As indicated in Section 6.2, processes for updating and distribution of this table to all Australian Government participants are under development.

An example extended FedLink lookup table and notes regarding the server behaviour rules is shown in Table 12.

Organisation	FedLink Connected	Domain Suffix	(Max) Classification of Information Accepted over FedLink	Status (Implemented Protective Markings?) ²⁷	Server Behaviour Notes
AAA	yes	@aaa.gov.au	UNCLASSIFIED	yes	Standard rules (inbound/outbound) apply
BBB	yes	@bbb.gov.au @bbb-bb.gov.au	UNCLASSIFIED IN-CONFIDENCE	yes yes	Standard rules (inbound/outbound) apply
CCC	yes	@ccc.gov.au	PROTECTED	no	FedLink Connected Originating agency - no protective marking applied to outbound or forwarded email At destination agency - inbound email accept all When sending to this agency, outbound rules apply
DDD	yes	@ddd.gov.au	PROTECTED	waiver	FedLink Connected Originating agency - no protective marking applied to outbound or forwarded email At destination agency - inbound email accept all When sending to this agency, outbound rules apply
EEE	no	@eee.gov.au	n/a	no	Non-Fedlink connected Originating agency - no protective marking applied to outbound or forwarded email At destination agency - inbound email accept all When sending to this agency, outbound rules apply (i.e. UNCLASSIFIED)
FFF	no	@fff.gov.au	n/a	waiver	Non-Fedlink connected Originating agency - no protective marking applied to outbound or forwarded email At destination agency - inbound email accept all

²⁷ Yes, No or Waiver – ‘no’ and ‘waiver’ processing rules are equivalent

Organisation	FedLink Connected	Domain Suffix	(Max) Classification of Information Accepted over FedLink	Status (Implemented Protective Markings?) ²⁷	Server Behaviour Notes
					When sending to this agency, outbound rules apply (i.e. UNCLASSIFIED)
GGG	no	@ggg.gov.au	n/a	yes	Non-Fedlink connected Originating agency - protective marking applied Standard inbound/outbound rules apply

Table 12 - Extended FedLink lookup table, showing the status of the implementation of protective markings

7 System Generated Email

As specified in ACSI 33, emails automatically generated by ICT systems should be marked with an appropriate protective marking. Example system generated emails include (but not limited to):

- email delivery receipts (Delivery Status Notification);
- application processing status messages (e.g. SAP generated email);
- notification of rejected or blocked emails; and
- system status messages (e.g. firewall, intrusion detection, DNS server messages).

8 Remote and Mobile Access to Email

Figure 3 shows a number of media, devices and mechanisms through which remote and/or mobile users may connect to their agency network to access email and other services. These users are essentially treated as if they were directly connected to the internal network. The physical and logical security of these remote access devices and the mechanisms that they use to remotely connect to the agency network, must be comparable to the overall classification of the agency network.

E.g. If an agency's physical environment is rated at the PROTECTED level, the mechanisms used to physically and logically secure the remote access device (e.g. laptop, PDA) and the mechanisms used to connect to the agency network over public infrastructure (e.g. dial-up, broadband, wireless) must also be at an equivalent PROTECTED level using appropriately endorsed products.²⁸

Agencies should also consider the direct (cable) connection of PDA devices to desktop computers, as these devices may be configured to automatically synchronise email (and other information) from the agency's internal email environment with the PDA device. Thus the PDA may hold security classified information and should be secured and handled accordingly. This is shown in Figure 4.

ACSI 33 provides the detailed requirements for the protection of portable computers and personal electronic devices.

²⁸ See Evaluated Products List at http://www.dsd.gov.au/infosec/evaluation_services/epl/epl.html

Appendix A – Sample Acceptable Use Email Guidelines

This section provides sample policy and guidelines only. Each agency must assess its own environment and gauge the applicability and suitability of the material provided.

Policy Statements

- All agency-originated emails that contain security classified information **MUST** be marked with a protective marking that identifies the maximum classification and set of caveats for the information in the body of the email and any attachments.
- All agency-originated emails that do not contain any classified information **MUST** be marked as UNCLASSIFIED.

User Guidelines

- *What is the policy requirement for the inclusion of protective markings in email?*

All email must contain a protective marking. This includes, but is not limited to, sending, replying, forwarding of email messages and meeting requests.

- *What is a protective marking?*

A protective marking is the combined set of Security Classification, Caveats and other indicators applied to information to indicate the information has been security classified indicating; whether it is national security or non-national security information; and the level of protective procedures that should be used over the information's lifetime.

- *How do you classify an email and attachments?*

Emails are classified using the same classification system used for paper based information as described in Part C of the Commonwealth Protective Security Manual. The protective marking applied to an email must reflect the highest classification of material contained in that email. E.g. If there are multiple attachments to an email, the protective marking applied must equal the highest classification of any of the attachments.

- *What is the format of a protective marking and where are they placed?*

The full format of the protective marking is described in the "Email Protective Marking Standard for the Australian Government". In its simplest form an unclassified email message would have [SEC=UNCLASSIFIED] added to the end of the 'Subject:' line such that the security classification is plainly visible to the recipient. Permitted security classifications for this agency are: IN-CONFIDENCE and PROTECTED.

- *How do you classify 'personal' emails?*

Personal or unofficial emails should be marked with the protective marking of [SEC=UNCLASSIFIED] added at the end of the 'Subject:' line.

- *What are the implications of over or under classification of email?*

The impact of over or under classification of email is the same as for paper based information (see PSM Part C). I.e. it will be subject to inappropriate handling, storage and transmission mechanisms between sites or to devices not designed or secured to receive that information.

- *What is the classification of email that may be transmitted on an agency's internal network?*

The <insert agency name> computing environment is classified to store and process information up to and including <insert network classification> material. Information rated above this classification MUST NOT be stored, processed or transmitted on the department's computing facilities.

- *What are the issues with sending security classified information to external addresses over the internet?*

The internet is not secure. Unless specific additional security measures are implemented, information transmitted across the internet may be intercepted, read and/or modified by a 3rd party. Security classified material MUST NOT be sent to external email addresses over the internet.

- *What is the classification of information that may be transmitted to a FedLink connected agency?*

FedLink is an Australian Government inter-agency secure communication facility that may be used to transmit information up to the PROTECTED classification. The classification of material that may be transmitted across FedLink is also dependent on what the recipient agency will accept. This may be lower than the PROTECTED rating of FedLink.

- *How do I find out what classification of information another agency will accept?*

The highest classification of information that may be transmitted across the internet is UNCLASSIFIED. The classification of material that an agency will accept over FedLink is available on the FedLink member's web site. If in doubt contact the IT Security Adviser (ITSA).

- *What is the classification of information that may be transmitted to/from a BlackBerry or any wireless connected device?*

Subject to specific Australian Government and agency policy and implementation standards, information that is UNCLASSIFIED,

IN-CONFIDENCE or RESTRICTED may be transmitted to/from a BlackBerry device.

- *Why was my email rejected?*

An email message may be rejected because:

- it contains an inappropriate (or incomplete) protective marking;
- the email classification exceeds the classification of the receiving system (including the <insert agency name> computing systems; or
- the classification of the email exceeds the classification of the path over which it would be transferred.

Review the email, its classification, the classification of the receiving system and the classification of the transfer path. If you are still not sure please contact the IT Security Adviser (ITSA).

- *What will happen if you attempt to send a message that exceeds the security rating of the recipient's email system?*

An email message may be rejected at the email gateway if:

- it contains an inappropriate (or incomplete) protective marking;
- the email classification exceeds the classification of the receiving system; or
- the classification of the email exceeds the classification of the path over which it would be transferred.

Review the email, its classification, the classification of the receiving system and the classification of the transfer path. If you are still not sure please contact the IT Security Adviser (ITSA).

- *What do I do if I receive a 'rejected email' message?*

If you receive an email 'rejected' message you should:

- Review the protective marking to ensure that it is correct; and
- Review the list of intended recipients to ensure that they can receive this level of security classified material.

Rejected emails are deleted and are NOT delivered.

If you are still not sure please contact the IT Security Adviser (ITSA).

- *Who is notified if an email is rejected?*

Rejected email notification (non-delivery) messages, are only sent to an internal agency address. I.e. to the email sender if the original email was addressed to an external user, or to the internal agency recipient if the original email was sent from outside of the agency. It is then up to the user who receives the rejected email notification to take appropriate action.

- *Are rejected emails delivered or logged?*

Rejected email messages are not delivered. Information describing the email, but not the email's content, is logged. Logged information may include, but is

not limited to: the sender and recipient addresses; subject, date and time of transmission and email size.

- *What should you do if you receive a message without a protective marking?*

Emails delivered without a protective marking would generally come from individuals, commercial organisations or non Australian Government agencies who are not bound by the requirements of the Protective Security Manual. You will need to add a protective marking if on-forwarding this email.

- *What should I do if forwarding an email that does not contain a protective marking to another user?*

You will need to classify the information contained in the email and add a protective marking before sending.

- *Is there a 'default' protective marking for email?*

No. As for paper based information, the author of the email must classify the information and add an appropriate protective marking.

Appendix B – Sample Email Rejected Messages

Outbound Message

Subject: Outbound email notification failure. [SEC=UNCLASSIFIED]

The <Insert agency name here> email gateway has received a message that it cannot deliver.

Generally emails are rejected because:

- they do not contain a valid protective marking; or
- the classification of the email exceeds the security rating of the recipient agency.

The message has been deleted from the system and has NOT been delivered to the intended recipients. Please review the security classification of this message and whether it is appropriate to send to the intended recipients.

For further assistance please contact <insert agency IT support group name>.

Email: <support_group_name>@<agency>.gov.au
Phone: (xx) xxxx xxxx

<Insert agency name here> email policy may be found at:
<http://<insert URL>>

User guidelines in relation to the classification of information may be found at:
<http://<insert URL>>

User guidelines in relation to the inclusion of protective markings in email may be found at:
<http://<insert URL>>

Blocked outbound email message details:

Subject: Protective Markings in an email's Subject field
Sender: First.Surname@agency.gov.au
Recipients: First.Surname@partner_agency.gov.au
Date:
Message Id:
Size:

Inbound Message

Subject: Inbound email notification failure [SEC=UNCLASSIFIED]

The <Insert agency name here> email gateway has received a message that it cannot deliver.

Generally emails are rejected because:

- they do not contain a valid protective marking; or
- the classification of the email exceeds the security rating of the recipient agency.

The message has been deleted from the system and the sender has NOT been notified of the delivery failure. If you believe that the message is legitimate please contact the sender and arrange a secure alternate means of delivery.

For further assistance please contact <insert agency IT support group name> or the email sender.

Email: <support_group_name>@<agency>.gov.au
Phone: (xx) xxxx xxxx

<Insert agency name here> email policy may be found at:
<http://<insert URL>>

User guidelines in relation to the classification of information may be found at:
<http://<insert URL>>

User guidelines in relation to the inclusion of protective markings in email may be found at:
<http://<insert URL>>

Rejected email message details:

Subject: Protective Markings in an email's Subject field
Sender: First.Surname@partner_agency.gov.au
Recipients: First.Surname@agency.gov.au
Date:
Message Id:
Size:

Appendix C – Glossary of Terms

Term	Meaning
ACSI 33	Australian Government Information and Communications Technology Security Manual. Published by the Defence Signals Directorate http://www.dsd.gov.au
Agency	An Australian Government or Commonwealth department.
BlackBerry	A system that can integrate with existing computer systems for wireless access to email and other corporate data. It can provide telephone, SMS, web browser, word processing and organiser functions.
Business partner	A commercial organisation that you exchange information with.
Caveat	A marking that indicates that the information has special requirements in addition to those indicated by the classification.
Defence-in-depth	An effective architecture for any information security program involves layering your security to provide multiple levels of defence. This is known as defence-in-depth. This includes separating your environment into digital zones and providing protection at all layers of your network, including the gateway, server and clients.
Email client	Mail User Agent, the software used to compose, send and read email.
Email gateway	A device or a system that receives email from a client system in one transport environment and transmits it to a server system in another transport environment.
ICON	Intra-government Communications Network
MIME	Multipurpose Internet Mail Extensions IETF standard for email content allowing multiple types of objects to be included as part of the body of an email message.
Other jurisdiction	A state, local or municipal government agency other than an Australian Government agency.
Partner agency	Another Australian Government agency that you exchange information with.
PDA	PDA (personal digital assistant) is a term for any small mobile hand-held device that provides computing and information storage and retrieval capabilities for personal or business use, often for keeping schedule calendars and address book information handy. The term handheld is a synonym. Many people use the name of one of the popular PDA products as a generic term. These include Hewlett-Packard's Palmtop (iPAQ) and 3Com's PalmPilot.
Protective marking	The combined set of Security Classification, Caveats and other indicators applied to information to indicate the information has been security classified; whether it is national security or non-national security information; and

Term	Meaning
	the level of protective procedures that should be used over the information's lifetime.
PSM	Protective Security Manual The principal means for disseminating Australian Government protective security policies, principles, standards and procedures to be followed by all Australian Government agencies for the protection of official resources.
RFC	Request for Comments The official publication channel for internet standards documents and other publications of the internet community.
Security classification	One of a standard set of terms that indicates the sensitivity of information and how it should be handled.

Table 13 - Glossary of Terms